



PROFESSIONAL SERVICES

INCIDENT RESPONSE
COMPUTER FORENSICS
APPLICATION SECURITY
NETWORK SECURITY
RESEARCH & DEVELOPMENT

EDUCATION

INCIDENT RESPONSE
MALWARE ANALYSIS
ADVANCED MALWARE ANALYSIS
NETWORK TRAFFIC ANALYSIS
WEB APPLICATION SECURITY
WIRELESS SECURITY

SOFTWARE

INTELLIGENT RESPONSE
FIRST RESPONSE
WEB HISTORIAN
RED CURTAIN



THREAT IDENTIFICATION PROGRAM™

MANDIANT's Threat Identification Program™ (TIP) addresses the current, advanced persistent threats targeting government agencies and the Defense Industrial Base. Powered by MANDIANT Intelligent Response™ (MIR), TIP combines our technology with our extensive knowledge of the advanced persistent threat into a solution that can “find evil” often missed while monitoring networks.

The perpetrators of these targeted threats possess an elevated understanding of victims' network topology, making the attackers appear like normal users and removing their need to scan for targets, or risk tripping internal alarms on the assailed network. The attackers escalate tactics only as necessary, and we have witnessed the sophistication of their efforts heighten as a direct result of specific countermeasures. Often, the attackers hide in plain sight by using custom malware and by securing valid credentials that allow lateral movement across the compromised organization.

Most organizations lack a centralized capability to identify and monitor constantly changing host-based signatures of compromise. As a result, we witness organizations spending significant amounts of money conducting tactical remediation before fully understanding the extent of the compromise or the adversary's traditional reactions to countermeasures.

For years, MANDIANT consultants have been in the trenches refining tactical countermeasures and strategic remediation plans to combat these persistent threats. As traditional prevention and detection technologies fail, organizations are being forced to operate in a state of continual compromise, while trying to stay ahead of the threat. At MANDIANT, we believe one answer to combat this challenge is adding enterprise incident response solutions — developed to evolve with the threat — to your network. Our experience has taught us that host-based monitoring and signature detection, in addition to network monitoring, are critical for protection against, and subsequent remediation of, targeted threats. TIP has proven successful in identifying malware that hides in routine network traffic or that lies dormant until required to maintain access to the network.

HOW DOES TIP WORK?

TIP is expert consulting focused on deploying a tactical enterprise detection and response capability across an organization's network and providing strategic remediation recommendations.

Utilizing MIR — an enterprise-grade incident response solution that provides the capacity to review thousands of systems in an expedited manner — we are able to look for specific indicators of compromise or investigate anomalous network activity from a host.

MANDIANT also offers the ability to expeditiously conduct static and dynamic analysis of hostile programs resulting in network and host-based indicators. MIR allows us to swiftly deploy these signatures throughout an enterprise and also provides a rapid response capability when network indicators identify suspicious hosts.

MANDIANT INTELLIGENT RESPONSE™

MIR is also a stand-alone product offering for those organizations that desire the internal capability to deploy an enterprise incident response solution with a host-based detection capability.

MIR is not an anti-virus, anti-spyware or intrusion detection solution. Because MIR has the technology to traverse a network — scanning for and collecting evidence of malware and other evil — it can detect when a system has been compromised, even if anti-virus programs do not have a signature.

WHO IS MANDIANT?

We are a company of consultants, authors, instructors and security experts. We have chased bad guys through the computer networks of *Fortune 500*, the defense industry, government agencies and the banks of the world. We can help “find evil and solve crime” through our products and services. We can also help you avoid it, through proactive services and education.

For more information about MANDIANT or to learn more about the Threat Identification Program, contact us at
1.800.647.7020 or
info@mandiant.com